THE RISING THREAT OF CHEAP AND SMALL COMMERCIAL DRONES TO US AND ALLIED FORCES: A CALL FOR ADVANCED C-UAS SYSTEMS

June 6, 2024 | Meryl Dzikansky

The rapid proliferation of cheap commercial drones, particularly those manufactured by Chinese companies, is creating a significant security challenge for military forces worldwide. These drones are becoming increasingly sophisticated and affordable, making them accessible to non-state actors and potential adversaries. This accessibility fuels a growing concern: the use of such Chinese-manufactured drones in operations specifically targeting US and allied forces.

In this article, we'll explore the implications of the widespread availability of commercial drones, the specific threats they pose to military security, and the various measures being implemented to mitigate these risks.

The Yokosuka Naval Base Incidents: A Breach in Security

The implications of the widespread availability of commercial drones are far-reaching and multifaceted, raising significant national security concerns. This threat became alarmingly apparent through a series of recent incidents at Yokosuka Naval Base in Japan, a critical hub for the US Navy's Seventh Fleet.

Two concerning drone incidents recently occurred at Yokosuka Naval Base.

May 2024: A drone flew undetected over the USS Ronald Reagan, a nuclear-powered aircraft carrier at the base. The incident, captured on video and shared on social media, exposed a vulnerability at the base and raised serious concerns regarding security at the base. The suspected operator, speculated to be a Chinese national, was never officially identified.

March 2024: A viral video emerged online showing footage of Japan's largest destroyer, the JS Izumo, docked at Yokosuka, was captured by a drone. This incident highlighted the potential for espionage using readily available drones.

These breaches underscore the potential for espionage and the ease with which hostile actors could exploit commercial drone technology to gather information on critical military infrastructure.

A Global Pattern of Drone Threats

The threat extends far beyond a single base. As highlighted in a recent opinion piece by Senators Jack Reed and Roger Wicker, the US and its allies face a growing vulnerability to low-flying drones.

Senators Reed and Wicker's report details troubling instances where low-altitude drones have infiltrated airspace:

Domestic Incursions: In the US, drones have disrupted commercial air traffic, crossed borders undetected, and were spotted over sensitive military installations.

Threat to Overseas Forces: US troops abroad are increasingly at risk. During the battle for Mosul, ISIS used commercial drones for offensive purposes, including dropping grenades and other explosives.

Weaponized Convenience

The affordability and ease of use of these drones make them particularly concerning, as they democratize access to sophisticated aerial technology that can be exploited for malicious purposes.

For example, Houthi rebels in Yemen have used weaponized drones, most likely with Chinese components, to target Saudi Arabian infrastructure. In 2022, the US Air Force reported encounters with unidentified drones fitting the Chinese-made profile operating near its Pacific region bases. These drones had high-resolution cameras and extended flight times, raising concerns about potential surveillance activities. Similar incidents have been documented by NATO forces in Europe.

Combating the Threat: A Multi-Layered Defense

The evolving threat necessitates a multi-layered Counter-Unmanned Aerial Systems (C-UAS) defense strategy. While traditional kinetic solutions like missiles and net guns may be effective in some situations, they often pose a risk of collateral damage and may not be suitable for all scenarios.

A crucial first line of defense lies in innovative, non-kinetic solutions like RF Cyber C-UAS systems. This technology leverages radio frequency (RF) signals to detect, identify, and neutralize unauthorized commercial drones. By taking control of such hostile drones, RF Cyber C-UAS systems effectively land or reroute them without physical engagement, minimizing risk and ensuring operational continuity. This ability to maintain operational continuity enhances situational awareness, responsiveness, and overall security posture.

The Urgent Need for Advanced C-UAS Systems

The strategic adversarial use of commercial drones, particularly those manufactured by Chinese companies, poses a significant and evolving threat to US and allied forces. The incidents highlighted here, from undetected drone overflights at Yokosuka Naval Base to weaponized drones used by insurgents, underscore the urgent need for robust and sophisticated counter-drone measures.

The growing threat demands a swift and decisive response. Implementing advanced C-UAS systems like RF Cyber C-UAS is essential to protect sensitive military assets and personnel. As the landscape of modern warfare evolves, so must defensive capabilities.

RF Cyber C-UAS systems can evolve in response to emerging commercial drone technologies, tactics, and vulnerabilities, ensuring that defense capabilities remain effective against the latest threats and providing long-term resilience and readiness against evolving adversarial tactics.